Is Your Endpoint Security Strategy Too Negative?

WHITE PAPER

NYOTRON
SECURING THE WORLD

Introduction

> *Computer security is definitely still a "hot topic". But why are we spending all this time and money and still having problems?*
> *- Marcus J. Ranum (2005)*[1]

Security remains one of today's hottest topics and an unsolved problem. Almost every week, there is a new crippling attack or data breach that we read about in the press. And this is just what had to be disclosed. What we read may just be the tip of the iceberg.

Until just a few years ago, endpoint security was relegated to a basic "antivirus checkbox". Most investment and innovation was focused on network layer defenses despite malicious actors using endpoints as an entry point into an organization for lateral movement, data staging as well as exfiltration.

Even though endpoint security has made a comeback in recent years, the war on malware is still being lost. This is a result of out-of-balance security approaches that rely mostly on Negative Security models to track down the bad and make limited use of Positive Security due to the limitations of first generation models. As malware authors continuously build up their arsenal of weapons, successful security strategies will need to embrace multi-layered defenses that include both Negative and Positive Security. A Second Generation OS-Centric Positive Security model represents a substantial improvement over first generation models to help you win the war on malware.

Resurgence of Endpoint Security

Just since 2015, venture capitalists have invested billions dollars in next-generation endpoint security technologies and these have gained significant market traction. Early adopters have been using these next-generation antivirus (NGAV) products for the past 2 to 3 years. While most vendors of these products have promised that their solutions based on machine learning (ML)/artificial intelligence (AI) are a "silver bullet" against malware, overall effectiveness has increased only marginally.

1 Ranum, Marcus, J. The Six Dumbest Ideas in Computer Security. 2015

Why aren't these new solutions delivering on their promise? The reality is that an organization is almost guaranteed to get infected due to the sheer number of new malware variants. For example, according to AV-TEST.org, there were more than 110 million new malware samples submitted in 2017.[2] Assuming an optimistic catch rate of 99.9%, 110,000 known malware variants were not detected. Moreover, since ML models are trained on known malware samples by definition; claims regarding their ability to catch new unknown threats simply aren't true.

There has been no noticeable improvement in endpoint security detection metrics and "AI fatigue" is setting in as public breaches and hacks grow despite the deployment of technologies such as Endpoint Detection and Response (EDR) and User and Entity Behavior Analytics (UEBA). Most organizations now assume that they have already been breached and are just trying to shorten discovery and limit impact. With an average time to identify the breach of 191 days and an average time to contain it of 66 days, we have a long way to go.[3]

Winning the War on Malware

> *Sometime around 1992 the amount of Badness in the Internet began to vastly outweigh the amount of Goodness.*
> *- Marcus J. Ranum (2005)[4]*

So, why more than two and a half decades later are we still chasing the "badness" and applying only the Negative Security model in the vast majority of security products? What if we become a bit more positive in the war on malware?

As a refresher, the Negative Security model defines what is disallowed (aka "bad") and allows everything else. This model is commonly used in antivirus (AV), host intrusion prevention system (HIPS), next-generation antivirus (NGAV) and data loss prevention (DLP) products, among others. Whereas the Positive Security model is one that defines what is allowed (aka "good" or "known") and rejects everything else.

2 https://www.av-test.org/en/statistics/malware/
3 Ponemon Institute, 2017 Cost of Data Breach Study, June 2017
4 Ranum, Marcus, J. The Six Dumbest Ideas in Computer Security. 2005

First Generation Positive Security Model

Whitelisting is the first generation of the Positive Security model for endpoints. It has been primarily successful among a limited number of highly sophisticated and very well-resourced Fortune 500 organizations. Why didn't it work out for everyone else? Unless deployed on a fixed workload device such as an ATM or a POS, or a web server, the inflexibility of whitelisting to meet the needs of today's dynamic application landscape can be crippling. The required maintenance overhead along with user dissatisfaction are pretty much unsustainable for a typical organization.

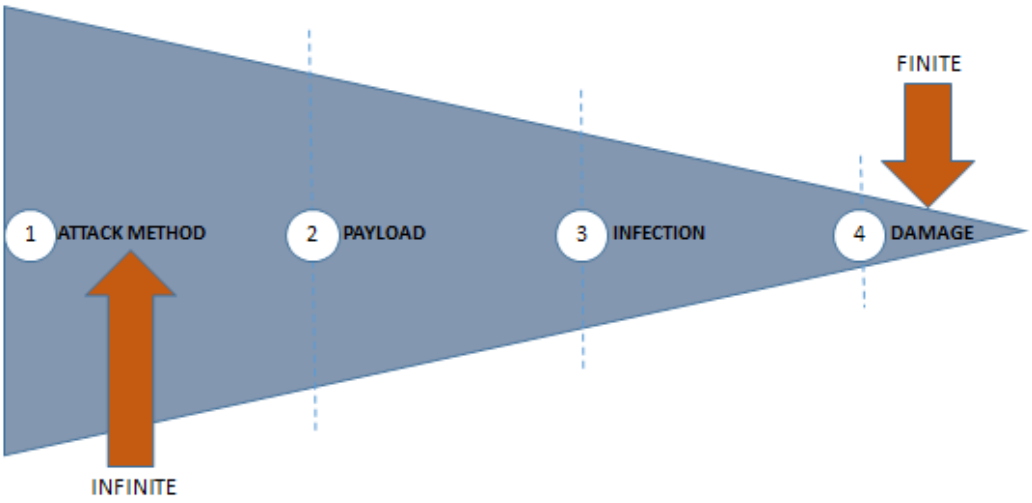

Figure 1: Attack Kill Chain

Second Generation Positive Security Model

To understand the Second Generation Positive Security Model, let's first look at the typical attack kill-chain in its simplified form—from Attack to Payload to Infection and finally to Damage as shown in Figure 1. The ways to attack an endpoint are practically infinite….OS and application vulnerabilities, exploits, social engineering attacks, Rubber Ducky and, most importantly, human ingenuity. Most security professionals agree that given enough time and resources, an attacker can breach any organization.

Unlike attack methods, intentions of the attacker in the damage stage remain a fairly static, finite set that is more or less limited to the following activities: data access and exfiltration (i.e. intellectual property, espionage), immediate monetary gain (i.e. ransomware) and data/system damage (i.e. wiper malware, hacktivism).

Second Generation or OS-Centric Positive Security focuses on the damage stage of the attack. Rather than looking at applications, this model looks at the actions that may cause system damage or data exfiltration. Additionally, the second generation of Positive Security avoids focusing on highly unpredictable user behavior that requires learning/baselining. Instead, it is a deterministic model that "pre-learns" or maps OS behavior. The second generation approach completely eliminates the massive management overhead that plagued the first generation approach (e.g. whitelisting) and, at the same time, ensures high levels of security.

Second Generation Positive Security Benefits

The benefits of the Second Generation or OS-Centric Positive Security include:

No patient zero required

Whether the malware is last year's or created just a minute ago doesn't matter. In fact, a second generation Positive Security solution does not care about the malware or the attack vector at all. It blocks any damage attempt at runtime.

No signatures or Indicators of Compromise (IOCs) needed

Heuristics, memory exploitation protection, deception, reputation analysis—all of these technologies are part of the Negative Security model to protect from polymorphic viruses. Since the Positive Security model does not "enumerate badness", signatures are completely irrelevant.

No learning/baselining or AI/ML algorithms

Security solutions using learning/baselining or AI/ML algorithms act only after detecting an unusual sequence of events—for example, the encryption of ten files within a short window of time. These solutions would prevent the encryption of additional files only after this point. In contrast, a second generation Positive Security product would prevent the encryption of the first file, resulting in zero damage. Although AI-based NGAV solutions are quite sophisticated and are trained on literally billions of known malware samples, training on the known does not necessarily protect you from the unknown.

Persistent security

Traditional security solutions work like gates—if attackers manage to pass through the gate they have practically unrestricted access to the endpoint and its data. This type of security is transient. On the other hand, Positive Security is persistent, analyzing every action every time forever.

Support for air-gapped environments and disconnected endpoints

Full protection capabilities are maintained whether the endpoint is connected or offline. The Positive Security-based solution does not rely on cloud-based threat intelligence to stop attacks and does need to send a previously unseen binary to a detonation sandbox somewhere in the cloud.

Protection of already infected endpoints

A Positive Security-based solution is fully preventative; it will block any attempt to cause damage to a system or data even if an endpoint was compromised prior to the installation of the product. And by the way, even unpatched (e.g. out of support) systems will be protected.

Fewer false positives

When you only operate on a few thousand state transitions of system events rather than on billions of files or millions of applications, false positives are greatly diminished.

More lightweight

Compared to solutions applying the Negative Security model, a solution based on the Positive Security model does not need to scan files and folders, update AV definitions or perform other resource-draining activities. Instead, the solution watches state transitions and compares them to a relatively small, finite set of normative transition sequences, resulting in no noticeable performance degradation.

Summary

> *The negative security model isn't bad; in fact, it's essential. It just isn't enough.*
> *- Kurt Roemer, Chief Security Strategist, Citrix*[5]

An OS-Centric Positive Security isn't a silver bullet, but it can be a tremendously valuable and complementary defense mechanism—your second or last line of defense. The majority of endpoint security solutions deployed today are based on the Negative Security model; so, it's time to add a Positive Security solution to strengthen your endpoint protection.

About Nyotron

Nyotron offers the last line of defense to help win the war on malware. Based on the industry's first OS-Centric Positive Security model that only allows legitimate operating system behavior, Nyotron prevents data exfiltration, corruption and other damage. Nyotron seamlessly complements existing endpoint security products with a future-proof solution providing protection from any attack vector without foreknowledge of an exploit. The company's headquarters is in Santa Clara, California, and R&D is in Israel. To learn more, visit www.nyotron.com.

5 Roemer, Kurt. Positive and Negative Security Models. Forbes. https://www.forbes.com/2009/05/05/citrix-security-roemer-technology-cio-network-citrix.html#206f3fad600a

NYOTRON
SECURING THE WORLD

2880 Lakeside Drive Suite 237
Santa Clara, CA 95054
+1 (408) 780-0750
www.nyotron.com